开源网安
SECZONE GROUP

安全自动化

趋势&解药

日程

应用安全认知

安全开发演化

安全开发现状

企业所面临的安全挑战

研发视角理解安全问题

S-SDLC & 讨论

信息安全


网络基础架构安全
网络路由交换
系统及服务
第三方软件
IT资产安全
网络路由交换
终端设备
系统及服务
第三方软件
社会工程学
欺诈
钓鱼
...
应用安全
自研软件安全
第三方安全依赖

应用安全解决什么？

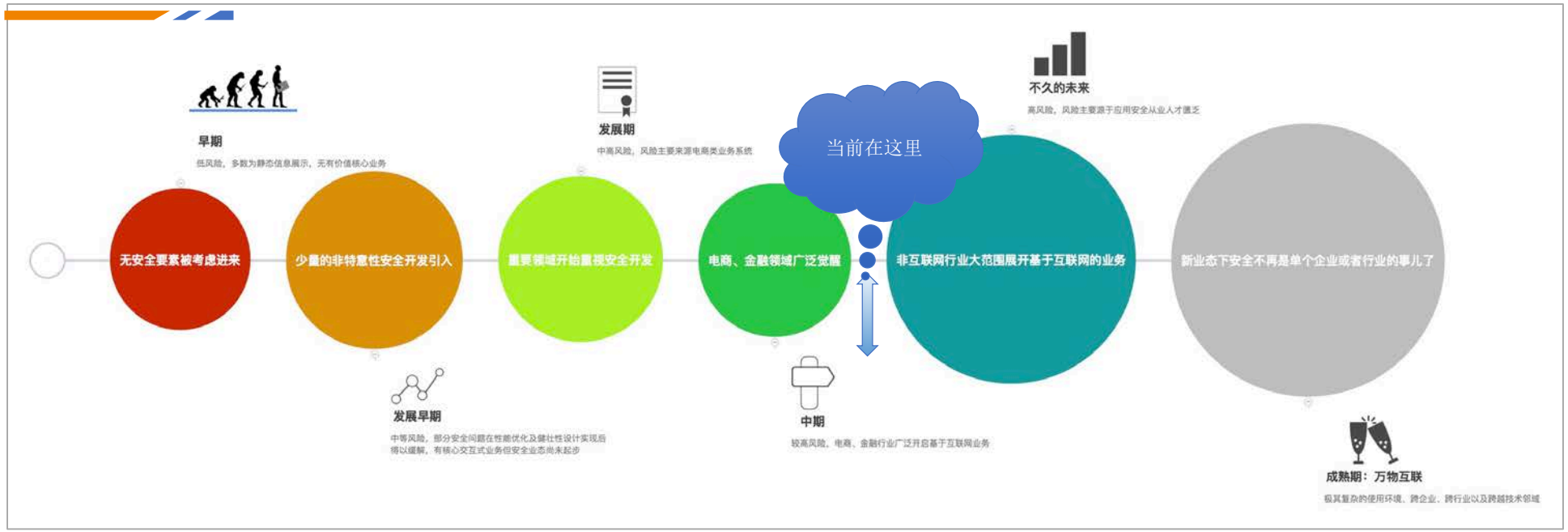
	极不可控 ☆☆☆★★	有限可控 ☆☆★★★	选择可控 ☆★★★★	自主可控 ★★★★★
信息安全	非传统安全	网络基础架构安全	IT资产安全	应用安全
	• 社会工程学 • 欺诈 • 钓鱼 • 物理安全	• 网络路由交换 • 系统及服务 • 第三方软件	• 网络路由交换 • 终端设备 • 系统及服务 • 第三方软件	• 自研软件安全 • 第三方安全依赖
人身安全	传统安全	环境安全	生活安全	身体安全
	• 恐怖袭击 • 突发战争	• 空气质量 • 地震	• 食品安全 • 交通安全	• 健康饮食 • 规律作息 • 适当运动

安全离我有多远？

日程

应用安全认知	安全开发演化	安全开发现状
企业所面临的安全挑战	研发视角理解安全问题	S-SDLC & 讨论

安全开发演化


早期
低风险，多数为静态信息展示，无有价值核心业务
无安全要素被考虑进来
少量的非特意性安全开发引入
发展早期
中等风险，部分安全问题在性能优化及健壮性设计实现后得以缓解，有核心交互式业务但安全业态尚未起步
发展期
中高风险，风险主要来源电商类业务系统
重要领域开始重视安全开发
电商、金融领域广泛觉醒
中期
较高风险，电商、金融行业广泛开启基于互联网业务
当前在这里
不久的未来
高风险，风险主要源于应用安全从业人才匮乏
非互联网行业大范围展开基于互联网的业务
新业态下安全不再是单个企业或者行业的事儿了
成熟期：万物互联
极其复杂的使用环境，跨企业，跨行业以及跨越技术邻域

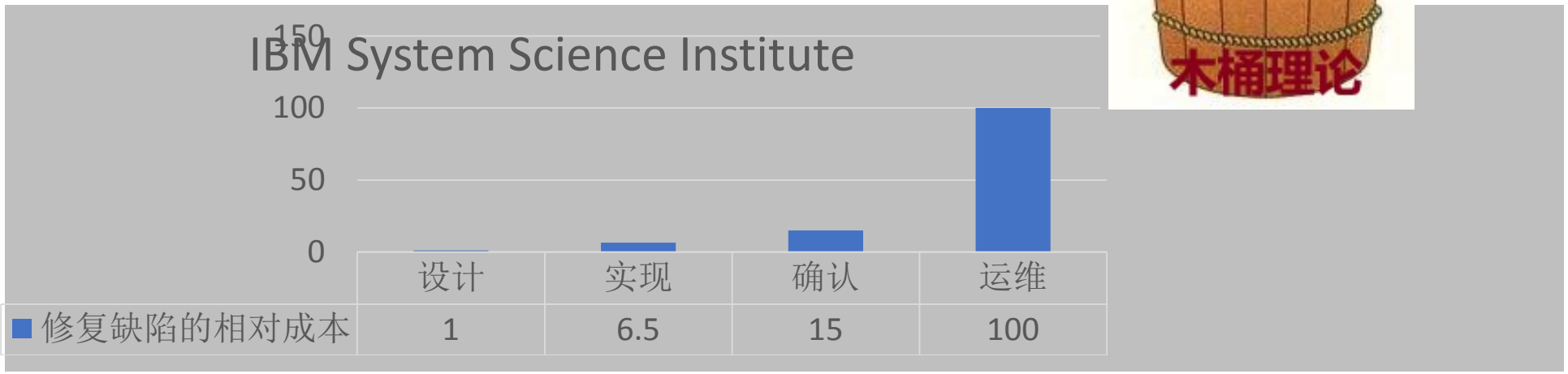
日程

应用安全认知	安全开发演化	安全开发现状
企业所面临的安全挑战	研发视角理解安全问题	S-SDLC & 讨论

安全开发现状


事件响应
需求
设计
实现
确认
部署、运维
架构审核
渗透测试


木桶理论


IBM System Science Institute
150
100
50
0
设计
实现
确认
运维
修复缺陷的相对成本
1
6.5
15
100

日程

应用安全认知	安全开发演化	安全开发现状
企业所面临的安全挑战	研发视角理解安全问题	S-SDLC & 讨论

安全是我们每一个头上的一把刀，随时都可能会掉下来，刺伤我们每一个人，我们的产品，我们的企业！~~

企业面临的安全挑战-高层领导

市场、安全组织对我们的产品报了N多安全漏洞，我希望这种现状需要快速缓解直至最终解决，主动出击，将问题扼杀在萌芽当中！，否则我们的客户将会逐步流失~

企业面临的安全挑战-商务销售

开源网安
SECZONE GROUP

我们正在着手解决，也组建了安全团队，但我们有产品交付的压力，我们需要更专业的安全人才的引入 ，我还需要增加研发人员来抵消安全实现的投入所带来的人力支出…

企业面临的安全挑战-CTO

有安全问题，当然要解决，问题是：
1. 请问题一次性告诉我，我好统筹解决
2. 谁能告诉我们如何解决才是最正确的，我经常遇到解决的问题被打回重新解决？
3. 我要保证产品交付，我不想做没有证据证明确实有安全问题的情况下来解决那些不明确的问题

企业面临的安全挑战-研发团队

绝大多数安全问题是由研发团队写代码写出来的，我们需要制订各种规范，让所有的人遵守：

- Java安全开发规范
- C、C++安全开发规范
- Struts安全开发规范
- Spring安全开发规范
- Web安全开发规范
- Desktop Software安全开发规范
- Server Side Software安全开发规范
- 敏感信息保护策略
- 加密算法安全使用指南
- ……

企业面临的安全挑战-安全团队

#1

最近 业界安全事件频发，我们公司全线产品的安全状态是什么？CTO/ CSO，明天给我一份安全现状评估报告给我！

高层领导

#2

老大，这些信息得从研发团队搜集，否则很难得到反应真实状况的数据 ！

CSO

#3

你们不是全程跟踪安全相关的事务的吗，怎么会没有数据？

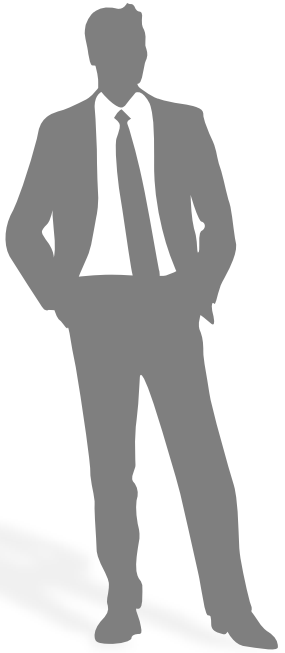
CTO

企业面临的安全挑战-CSO/CTO/Highlevel

企业面临的安全挑战-开发流程

Agile:
安全开发流程涉及的工作刚展开，一个Sprint已经结束了~~

Waterfall:
研发团队总是习惯于将安全问题放到Release的末尾，最终如果有产品交付时间冲突，安全将会被『和谐』掉，最终成为烂尾楼~~



企业面临的安全挑战-工具的利与弊

日程

应用安全认知	安全开发演化	安全开发现状
企业所面临的安全挑战	研发视角理解安全问题	S-SDLC & 讨论

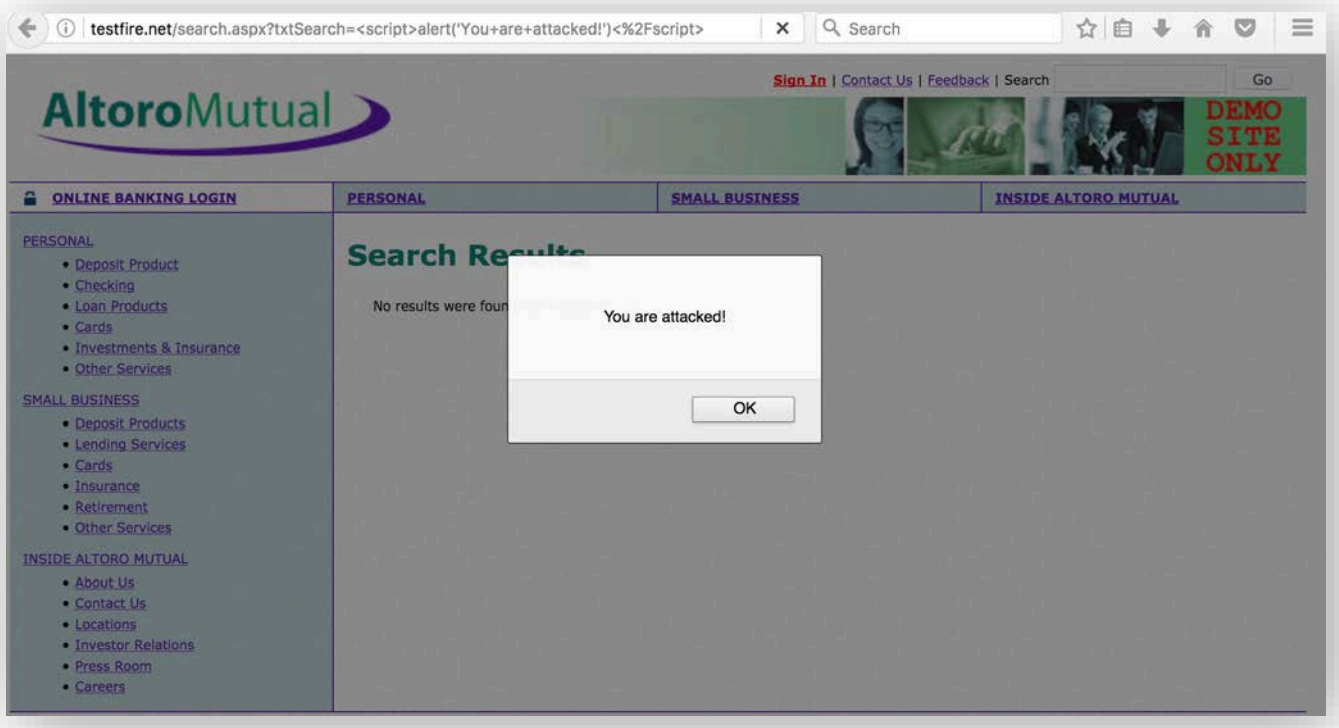
从研发的视角理解安全问题--

别让各种安全名词扰乱了方寸

1. 肉鸡
2. 木马
3. 网页木马
4. 挂马
5. 后门
6. rootkit:rootkit
7. IPC$
8. 弱口令
9. 默认共享
10. shell
11. WebShell
12. 溢出
13. 注入
14. 注入点
15. 劫持
16. 提权
17. 端口
18. 3389、4899肉鸡
19. 免杀
20. 加壳
21. 花指令
19. 20. 21……

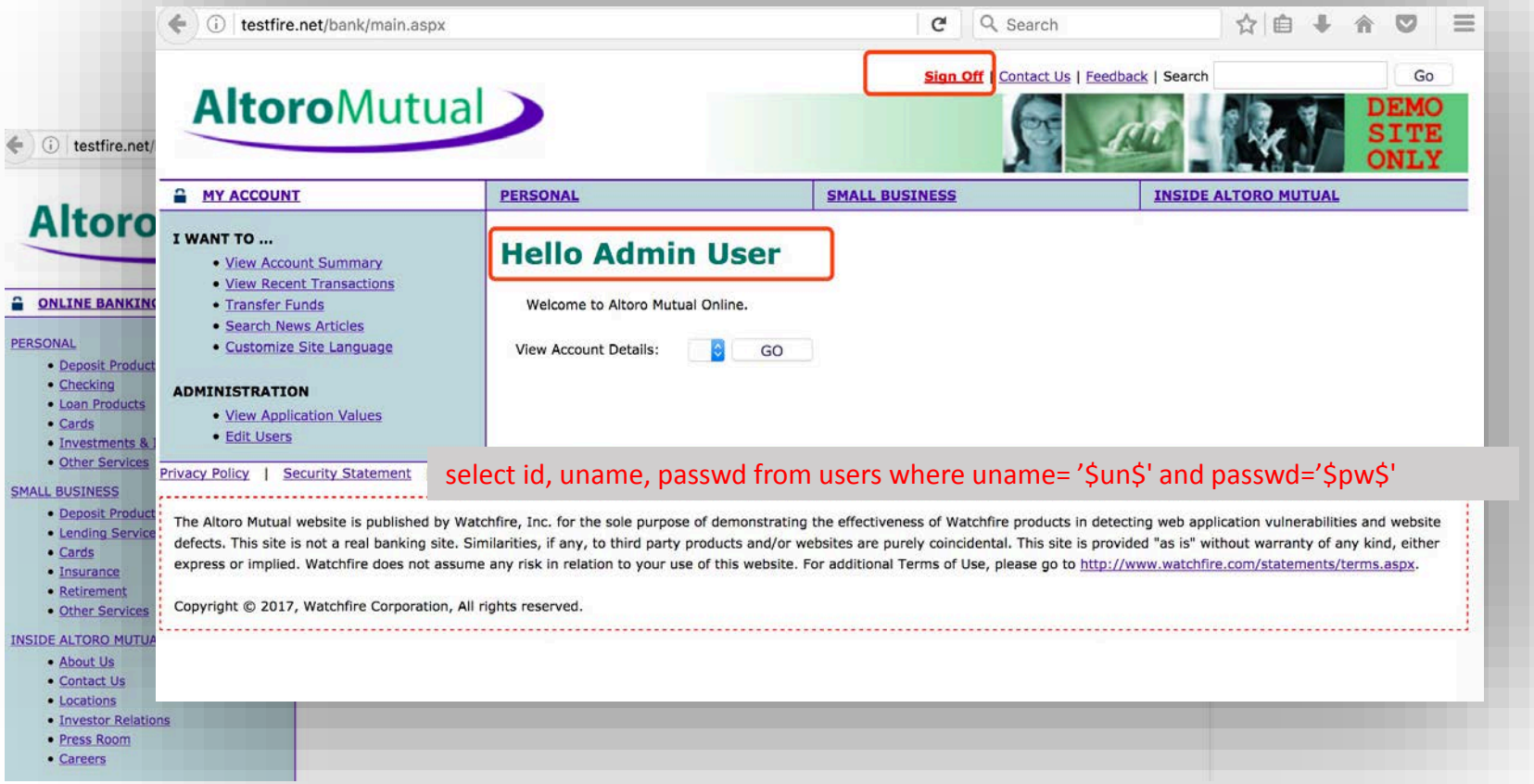
从研发的视角理解安全问题

XSS



从研发的视角理解安全问题

SQL Injection



从研发的视角理解安全问题

SDLC

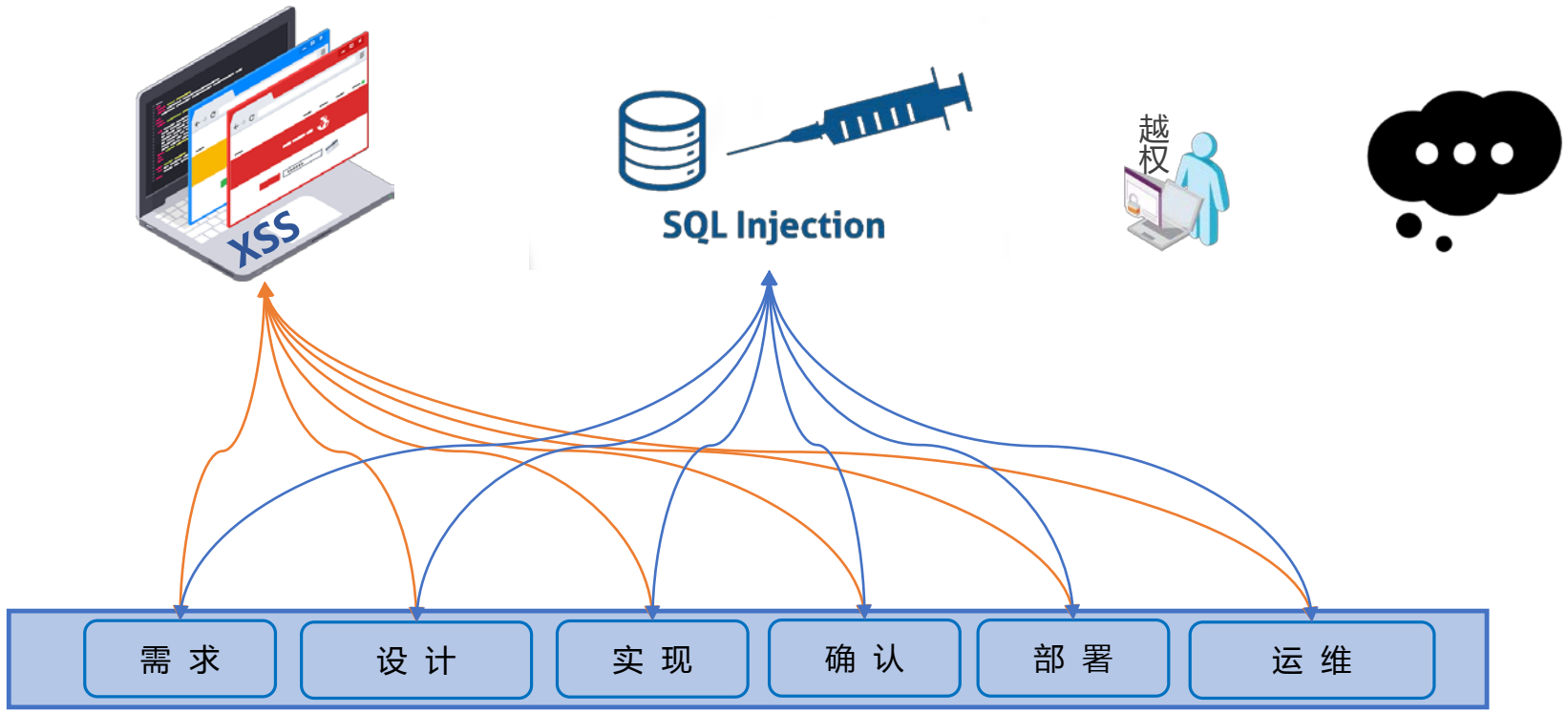


Table of Content

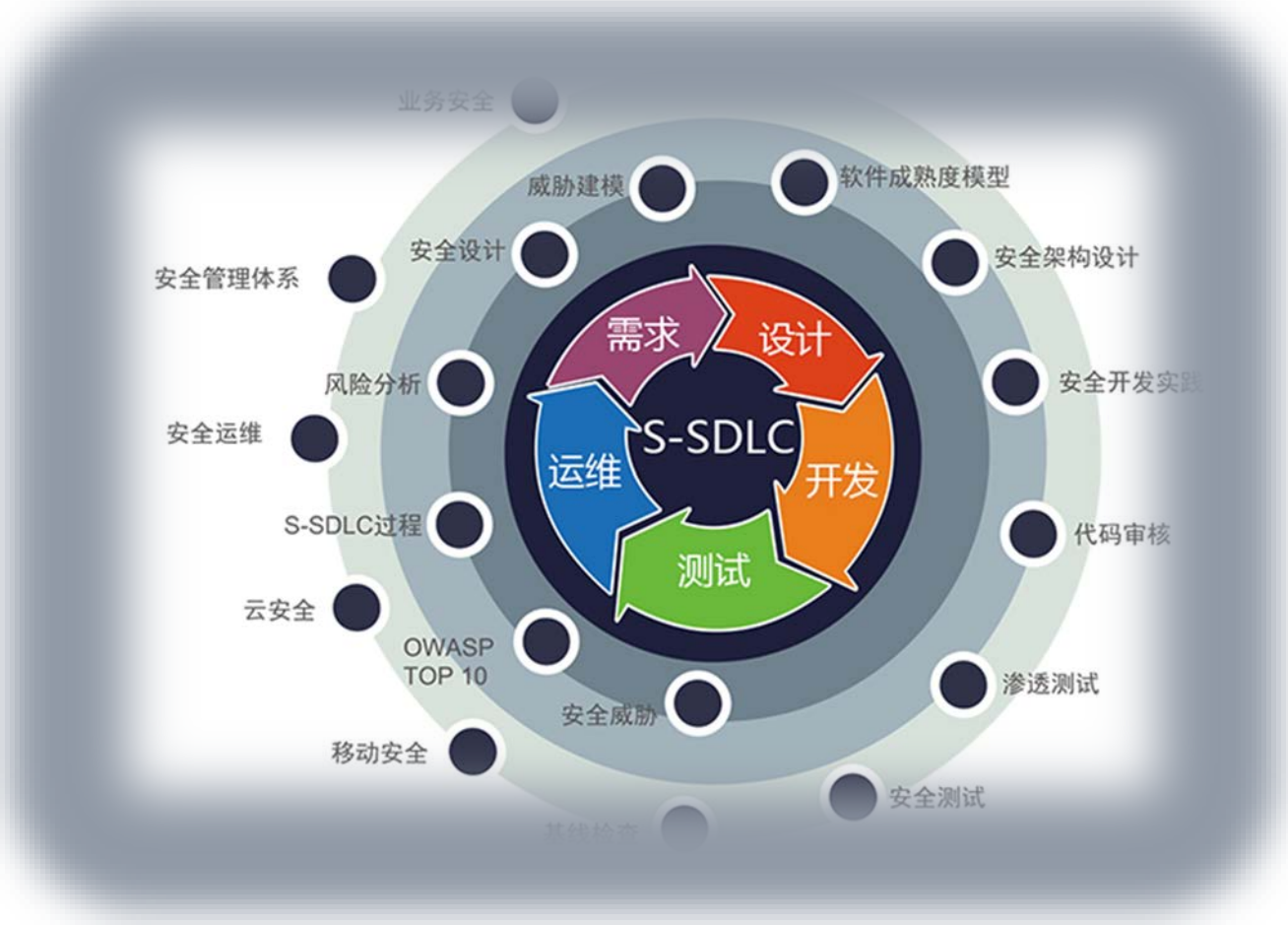
I	**Programming Security**
I.1	Does your task add or modify a text inpu
	If yes:
I.1.1	Have you specified the maximum input fields?
I.1.2	Do you want to allow HTML in you
	If yes:
I.1.2.1	Does your input field allow th tags?
	If yes:
I.1.2.1.1	Does your task allow ar hyperlinks?
	If yes:
I.1.2.1.1.1	Have you made the link will oper window?
I.1.2.1.2	Does your task allow ar embedding of ActiveX c (unusual)

II	**Authentication & Access Control**
II.1	Does your task add a new web page?
II.2	Does your task allow communication with
II.3	Does your task require adding or modifyi information?
II.4	Does your task modify user's access cont
II.5	Does your task allow access to other onli

III	**Privacy**		
III.1	Does your task require collecting, using, **data**[v]?		
	If yes:		
III.1.1	Did you outline important business reasons for doing so?	_	_
III.2	Does your task require collecting, using, storing or transmitting **personal data**[vi]?	_	_
	If yes:		
III.2.1	Did you outline important business reasons for doing so?	_	_
III.2.2	Does the user clearly and unambiguously consent to which personal data Cisco collects, uses, stores or transmits?	_	_
III.2.3	Does your task ensure access control to personal data?	_	_
III.2.4	Does your task ensure the user can update her personal data?	_	_
III.2.5	Does your task ensure that personal data is retained no longer than necessary for the stated business purpose?	_	_

- 1.安全需求识别
- 2. 安全设计
  - 2.1 输入校验
  - 2.2 敏感信息处理
  - 2.3 访问控制
  - 2.4 输出编码
  - 2.5 参数化sql
  - 2.6 身份验证
- 3. 安全设计检查清单
  - 3.1 输入校验设计检查清单
  - 3.2 敏感信息处理设计检查清单
  - 3.3 访问控制
  - 3.4 输出编码
  - 3.5 参数化sql
  - 3.6 身份验证

S-SDCLC



软件安全的终极解决方案-S-SDLC

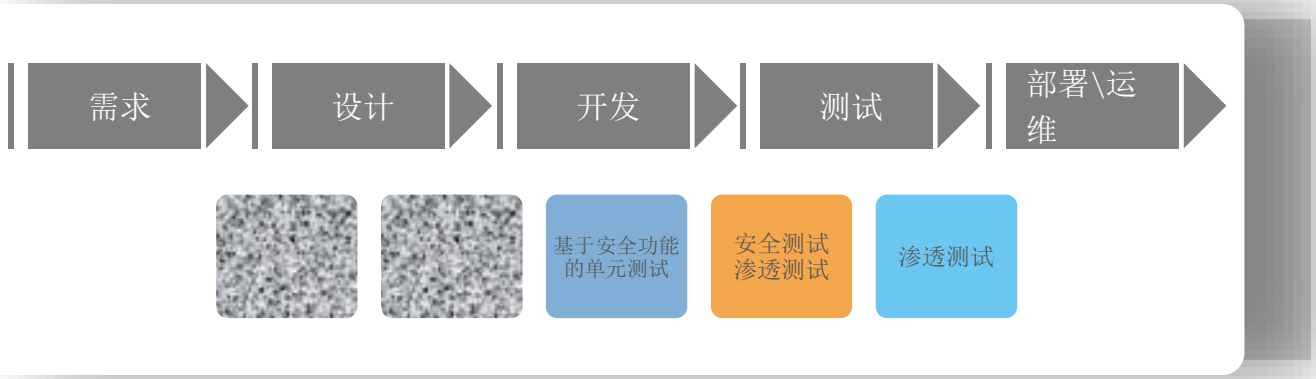
日程

应用安全认知	安全开发演化	安全开发现状
企业所面临的安全挑战	研发视角理解安全问题	S-SDLC & 讨论

初识S-SDLC

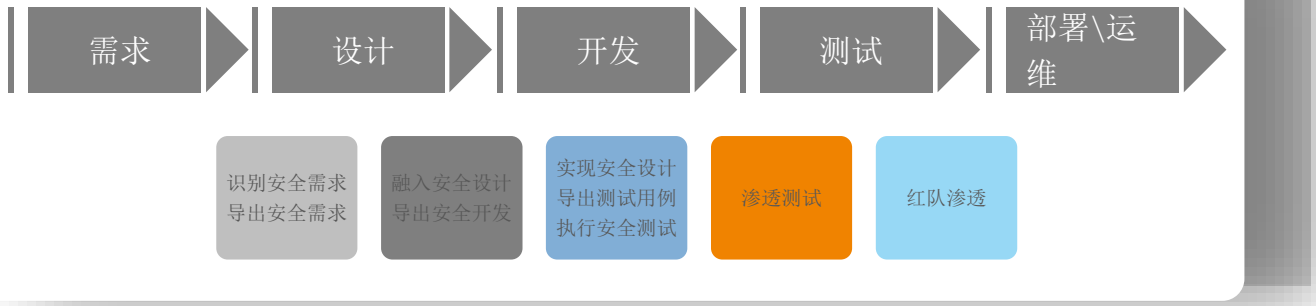
传统的

安全开发过程

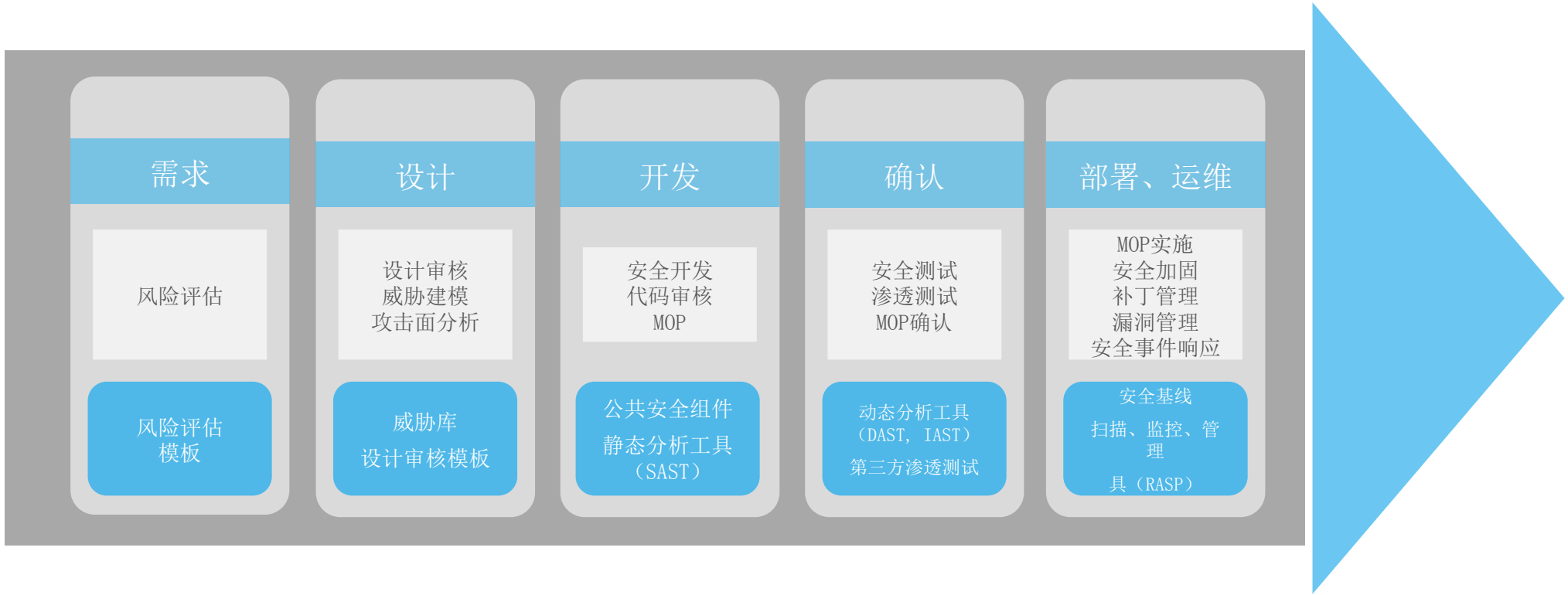


S-SDLC

安全开发过程

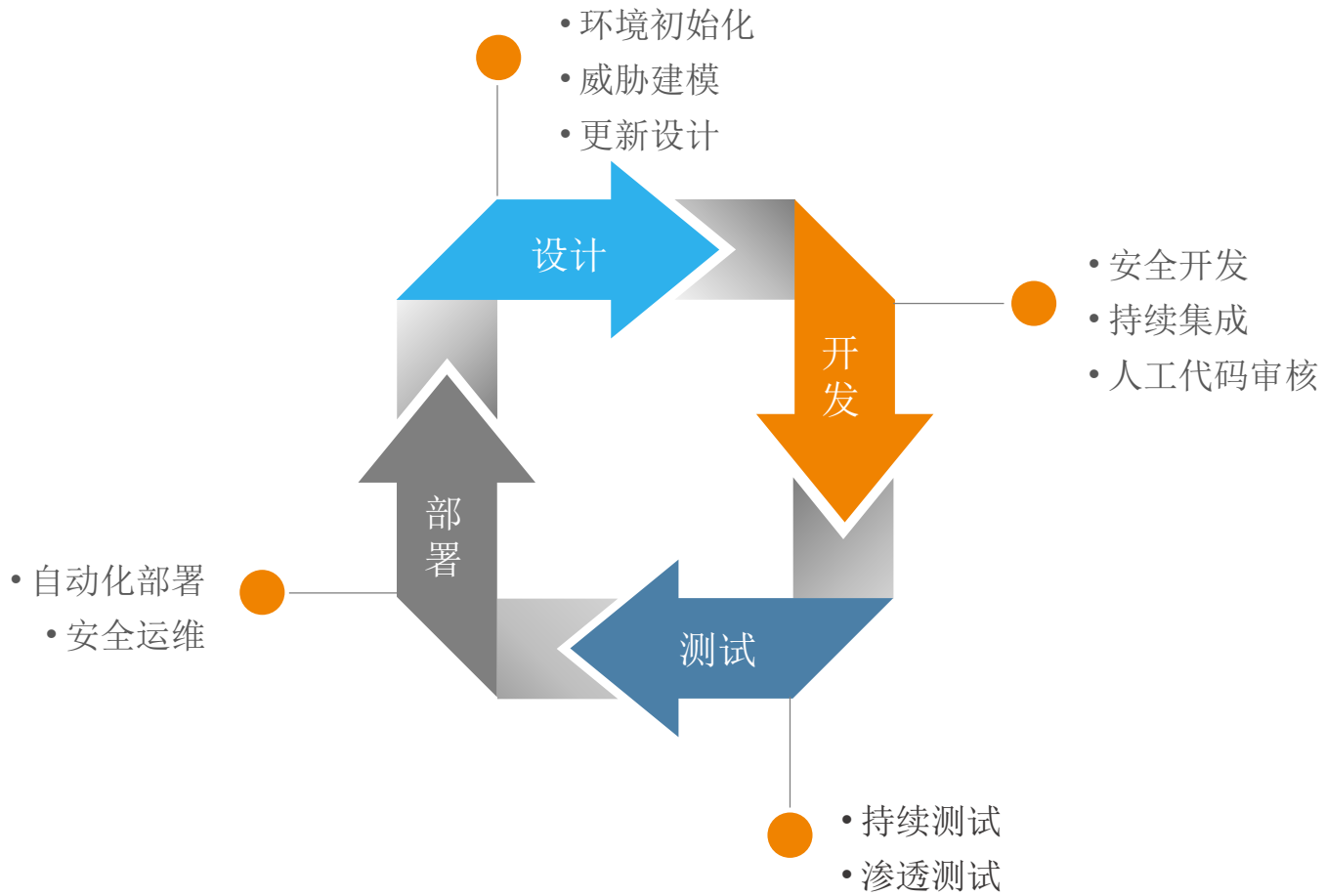


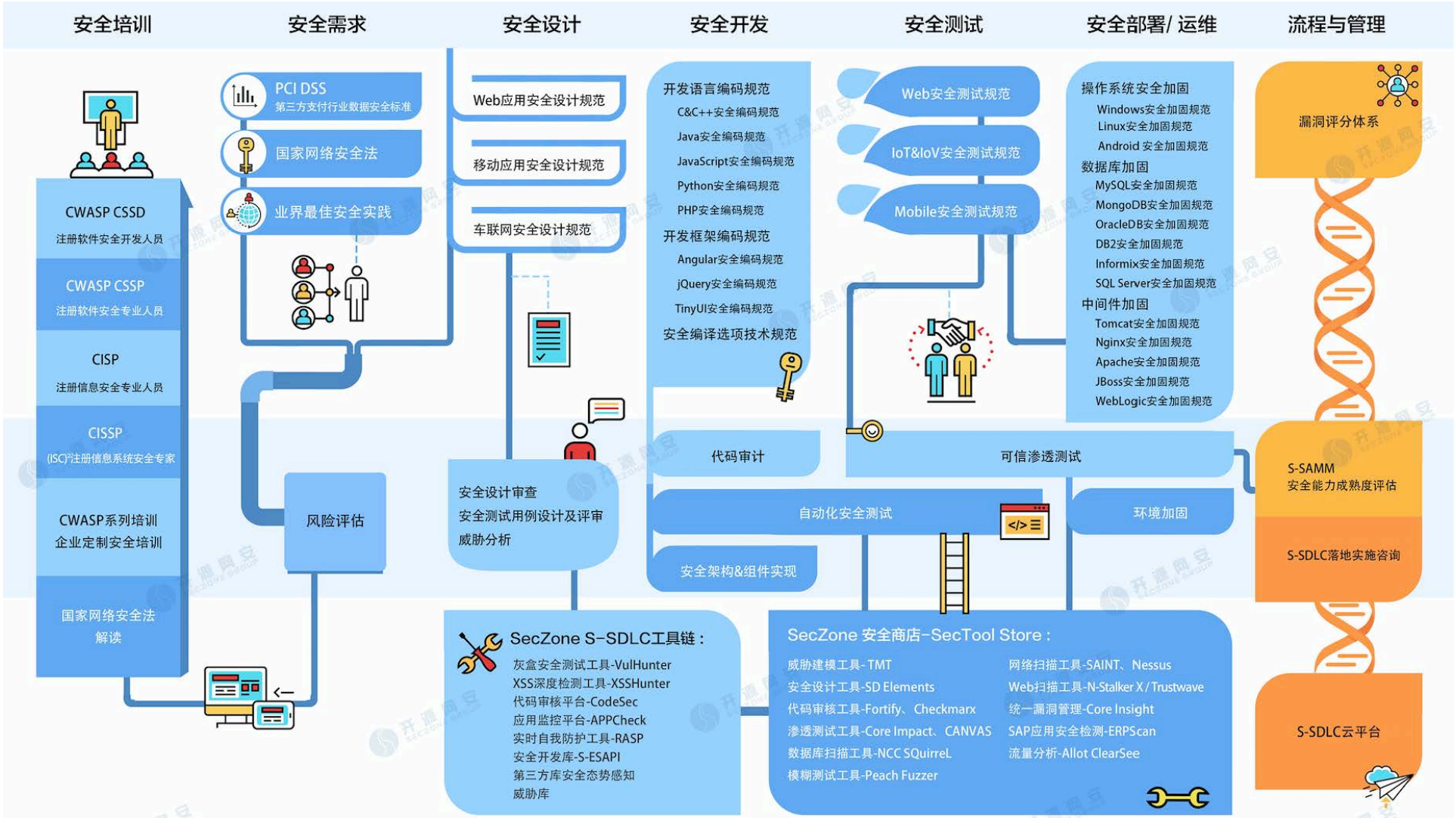
理解S-SDLC


需求
风险评估
风险评估
模板
设计
设计审核
威胁建模
攻击面分析
威胁库
设计审核模板
开发
安全开发
代码审核
MOP
公共安全组件
静态分析工具
（SAST）
确认
安全测试
渗透测试
MOP确认
动态分析工具
（DAST，IAST）
第三方渗透测试
部署、运维
MOP实施
安全加固
补丁管理
漏洞管理
安全事件响应
安全基线
扫描、监控、管理
具（RASP）

S-SDLC流程关键要素

S-SDLC流程与敏捷开发




安全培训
安全需求
安全设计
安全开发
安全测试
安全部署/ 运维
流程与管理
CWASP CSSD
注册软件安全开发人员
CWASP CSSP
注册软件安全专业人员
CISP
注册信息安全专业人员
CISSP
(ISC)²注册信息系统安全专家
CWASP系列培训
企业定制安全培训
国家网络安全法
解读
PCI DSS
第三方支付行业数据安全标准
国家网络安全法
业界最佳安全实践
风险评估
Web应用安全设计规范
移动应用安全设计规范
车联网安全设计规范
安全设计审查
安全测试用例设计及评审
威胁分析
开发语言编码规范
C&C++安全编码规范
Java安全编码规范
JavaScript安全编码规范
Python安全编码规范
PHP安全编码规范
开发框架编码规范
Angular安全编码规范
jQuery安全编码规范
TinyUI安全编码规范
安全编译选项技术规范
代码审计
安全架构&组件实现
Web安全测试规范
IoT&IoV安全测试规范
Mobile安全测试规范
可信渗透测试
自动化安全测试
操作系统安全加固
Windows安全加固规范
Linux安全加固规范
Android 安全加固规范
数据库加固
MySQL安全加固规范
MongoDB安全加固规范
OracleDB安全加固规范
DB2安全加固规范
Informix安全加固规范
SQL Server安全加固规范
中间件加固
Tomcat安全加固规范
Nginx安全加固规范
Apache安全加固规范
JBoss安全加固规范
WebLogic安全加固规范
环境加固
漏洞评分体系
S-SAMM
安全能力成熟度评估
S-SDLC落地实施咨询
S-SDLC云平台
SecZone S-SDLC工具链：
灰盒安全测试工具-VulHunter
XSS深度检测工具-XSSHunter
代码审核平台-CodeSec
应用监控平台-APPCheck
实时自我防护工具-RASP
安全开发库-S-ESAPI
第三方库安全态势感知
威胁库
SecZone 安全商店-SecTool Store：
威胁建模工具- TMT
安全设计工具-SD Elements
代码审核工具-Fortify、Checkmarx
渗透测试工具-Core Impact、CANVAS
数据库扫描工具-NCC SQuirreL
模糊测试工具-Peach Fuzzer
网络扫描工具-SAINT、Nessus
Web扫描工具-N-Stalker X / Trustwave
统一漏洞管理-Core Insight
SAP应用安全检测-ERPScan
流量分析-Allot ClearSee


可是臣妾做不到啊

9 SAST白盒工具落地不了...

8 要干活！！！

7 还要保障产品安全！！！

4 国外工具不会用！

5 英文报告看不懂！

6 错误不会修复！！

3 没人懂代码安全！！！

2 没钱请专家！！！

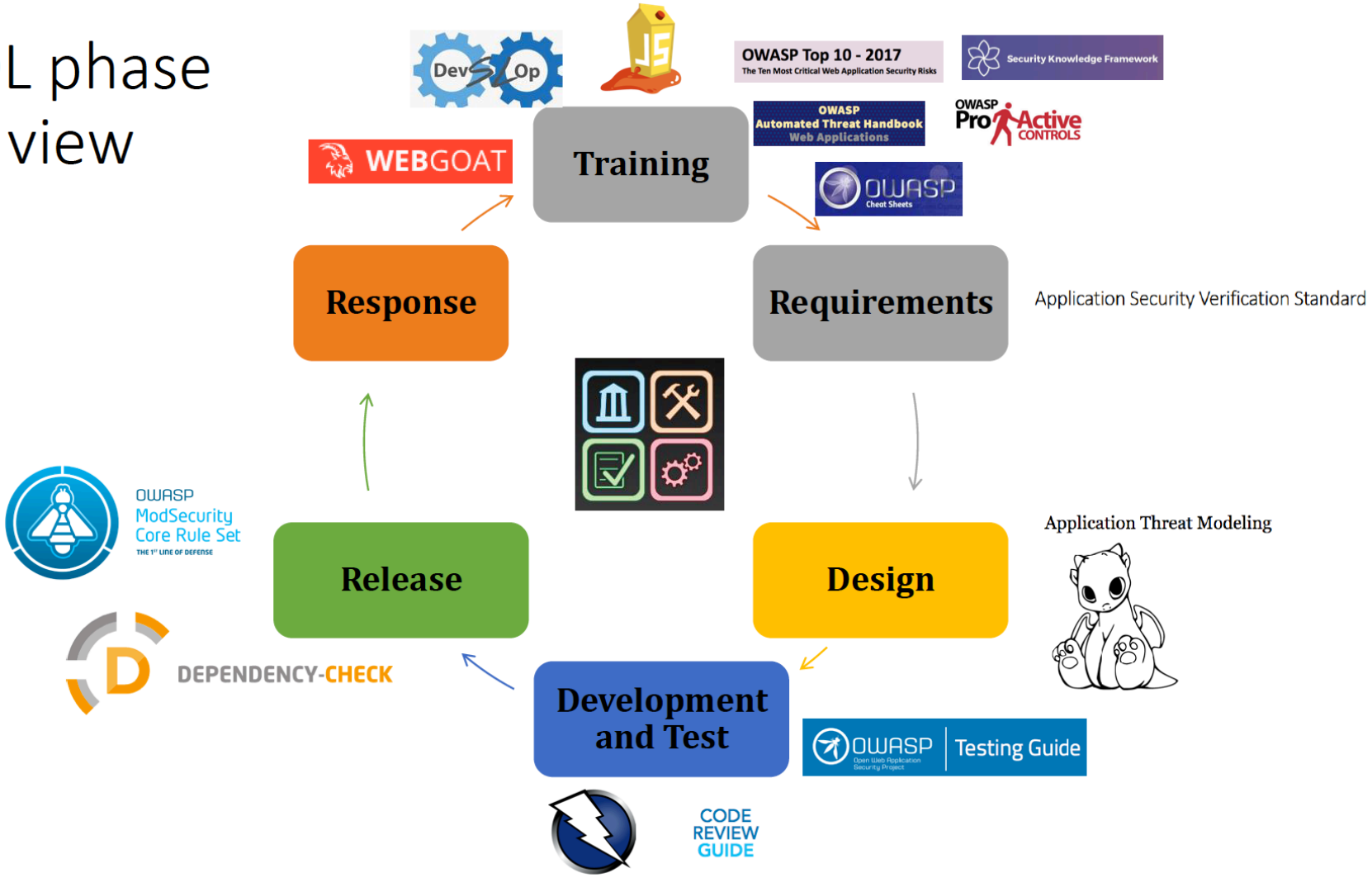
1 安全测试没时间！！！

思考-实践

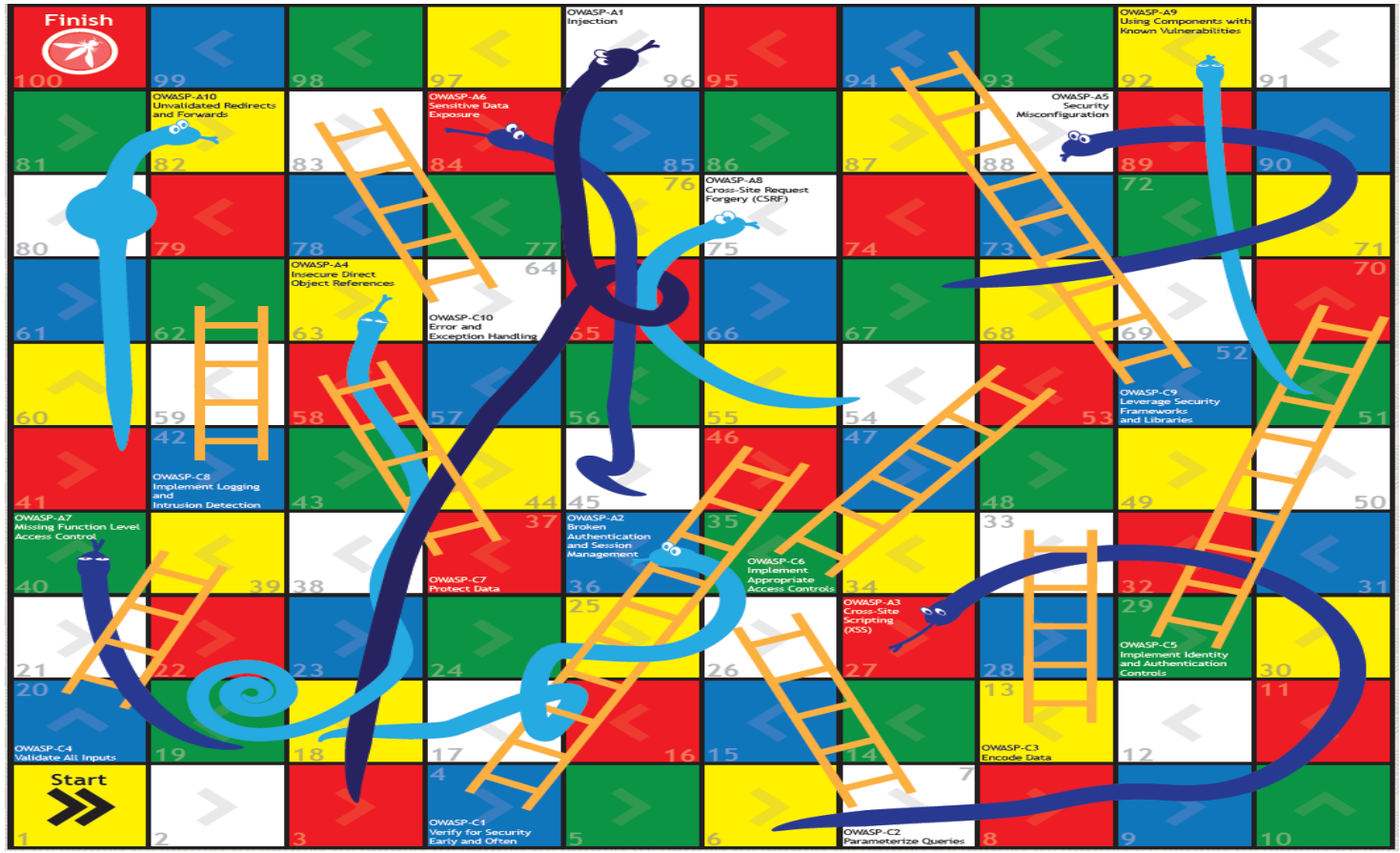
- 企业必须自上而下推行S-SDLC实施，且有相应的组织结构支撑
- S-SDLC要与企业的质量管理体系相结合
- 建立合适的人员培训体系
- 用度量体系将S-SDLC实施效果可视化
- 产品的安全目标决定S-SDLC的过程
- 威胁模型可以使产品避免大的设计风险
- 安全特性组件化可尽量避免编码漏洞
- 管理第三方软件的风险
- 安全服务化和自动化是实施DevSecOps的基础
- S-SDLC工具链


Gartner

SDL phase view



工具1 – Snake&Ladder

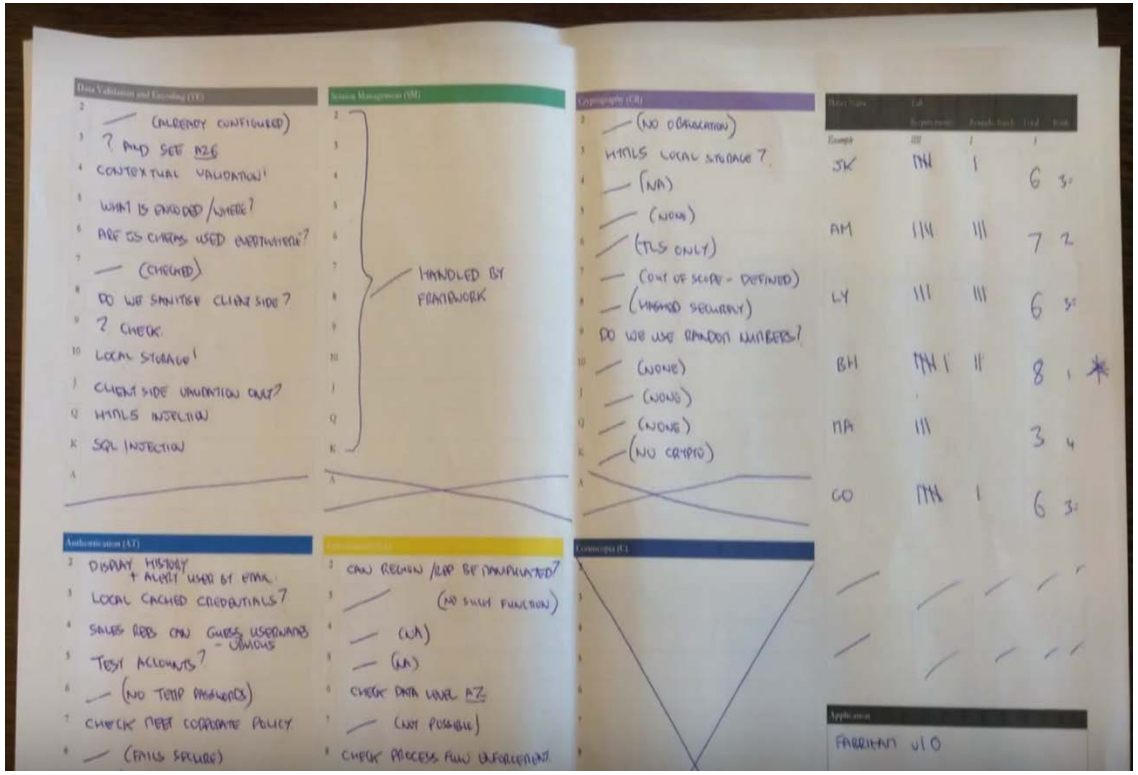


工具2 - ASVS

		1	2	3
V9.1	Verify that all forms containing sensitive information have disabled client side caching, including autocomplete features.	✔	✔	✔
V9.2	Verify that the list of sensitive data processed by this application is identified, and that there is an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit). Verify that this policy is properly enforced.			✔
V9.3	Verify that all sensitive data is sent to the server in the HTTP message body (i.e., URL parameters are never used to send sensitive data).	✔	✔	✔
V9.4	Verify that all cached or temporary copies of sensitive data sent to the client are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).		✔	✔
V9.5	Verify that all cached or temporary copies of sensitive data stored on the server are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.		✔	✔
V9.6	Verify that there is a method to remove each type of sensitive data from the application at the end of its required retention period.			✔

1. 开发者可用来做指导
2. 安全人员可以用来检查
3. 外包作为验收标准

工具3 - Cornucopias



1. Gamification
2. OWASP SCP/ASVS/Testing guide
3. 6 suites * 13 cards
   - Data validation and encoding
   - Authentication
   - Session management
   - Authorization
   - Cryptography
   - Cornucopia

https://www.youtube.com/watch?v=i5Y0akWj31k

工具4 - OWASP Dependency

Collect all dependencies → Identify CPE → Search vulnerabilities from NVD → CVE Report

DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

Project: Demo Insecure Project

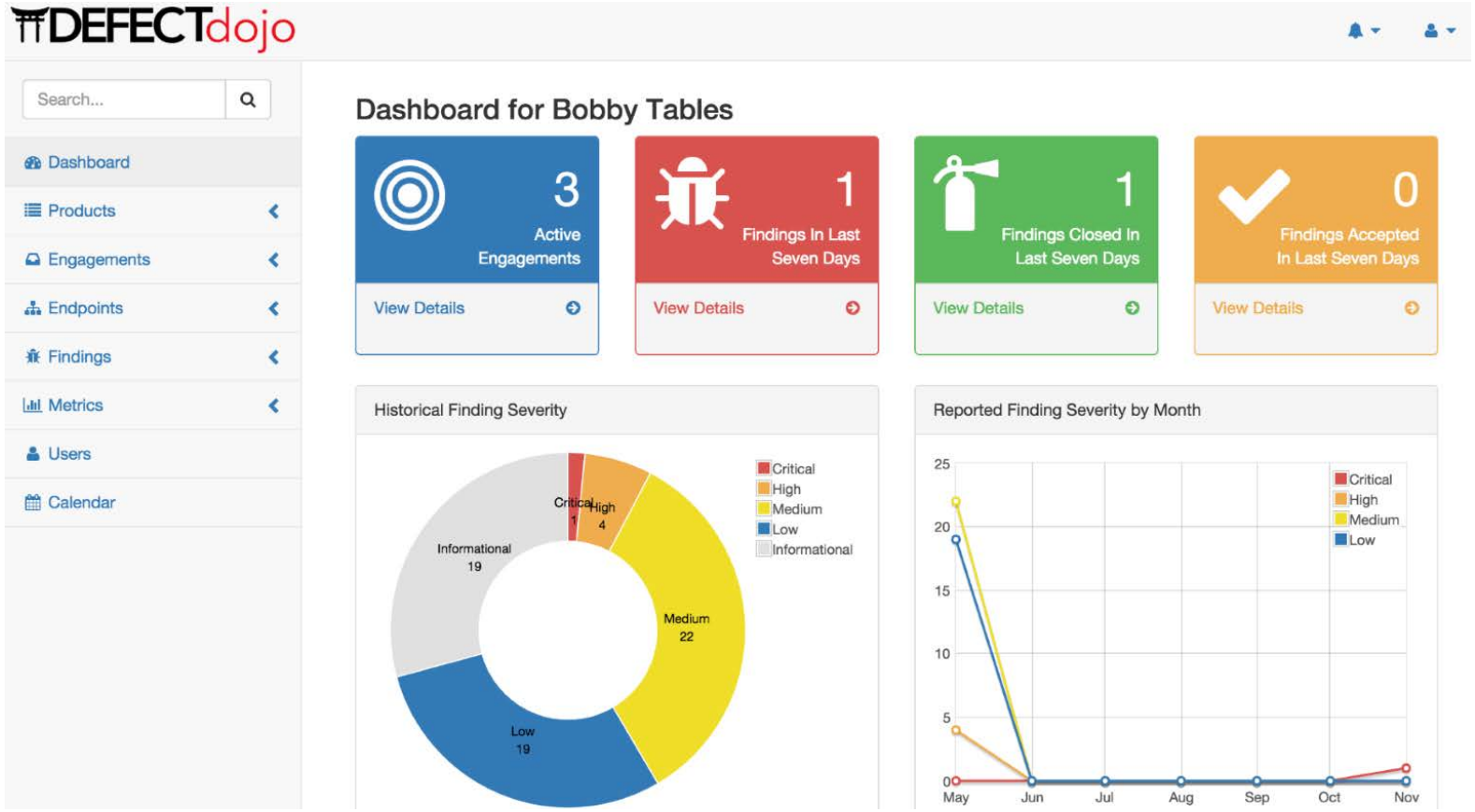
Scan Information (show all):

- *dependency-check version*: 1.3.1
- *Report Generated On*: Nov 3, 2015 at 23:20:33 EST
- *Dependencies Scanned*: 14
- *Vulnerable Dependencies*: 3
- *Vulnerabilities Found*: 13
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
commons-fileupload-1.3.jar	cpe:/a:apache:commons_fileupload:1.3	commons-fileupload:commons-fileupload:1.3	Medium	1	HIGHEST	29
struts2-core-2.3.15.3.jar	cpe:/a:apache:struts:2.3.15.3	org.apache.struts:struts2-core:2.3.15.3	High	6	HIGHEST	25

工具5 - OWASP Defect Dojo



Missing pieces

- No options for SAST or IAST
- A dashboard to track everything (requirements management, activities, releases, metrics)

公司简介 ABOUT US

创新 融合 开拓

SecZone

SecZone成立于2013年5月，是国内软件安全行业创领者和领先的软件安全开发生命周期（S-SDLC）解决方案提供商，专注于软件安全领域的技术研究。SecZone团队由来自思科、微软、惠普、Google、华为等行业顶级的安全专家组成，团队成员从业经验均为10年以上。SecZone总部在深圳，同时在北京、广州、武汉、合肥、成都、南宁设有分支机构。

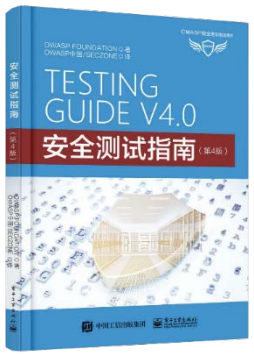
SecZone始终以自主创新为发展源动力，以S-SDLC解决方案为核心，以S-SDLC平台为载体，向不同行业的客户提供覆盖软件开发全生命周期的软件安全开发咨询和落地服务，包括但不限于安全开发培训、安全需求识别、安全架构设计、安全代码实现、安全确认、安全审核及安全运营的完整业务生态，同时提供配套的工具链支持。帮助客户提升软件安全开发能力，构建安全可靠的软件产品。

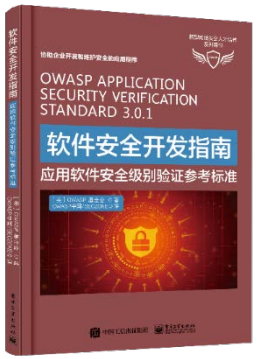
未来

SecZone将持续聚焦软件安全领域，努力成为全球软件安全领域极具竞争力的领导品牌。

SecZone

SecZone优势





OWASP
Open Web Application
Security Project

应用安全联盟
互联网安全研究中心

VulHunter自动化灰盒安全测试工具

VulHunter产品——VulHunter简介

- VulHunter是国内首款自主知识产品的新一代代码审计、安全测试和第三方软件检测产品
- 由国内领先的软件安全开发生命周期（S-SDLC）解决方案提供商SecZone研发，拥有自主知识产权
- 在开发和测试阶段均可以无缝集成，“零成本”实现代码审计、安全测试和第三方软件检测

代码审计
第三方软件检测

安全
测试

思考-工具

技术比较	SecZone VulHunter	SAST	DAST
开发流程集成度	无缝集成开发和测试阶段，零成本完成安全测试	开发阶段，成本较高	测试阶段，成本较高
误报率	较低	较高	最低
测试覆盖度	高，受功能测试覆盖度保障	高	低
检测速度	准实时，和应用程序复杂度无关	非实时，和应用程序复杂度相关，随代码量增加呈指数增长	非实时，和应用程序复杂度相关，程序越复杂，测试用例越多，速度越慢
支持检测的漏洞类型	最多	部分	部分
第三方软件及其漏洞检测	完全支持	有限支持	非常有限
漏洞信息丰富程度	动态数据流+请求和响应信息+配置文件+...	只有静态数据流	只有请求和响应信息
“脏”数据影响	无	无	有
多项目并发	完全支持，可以同时对100+个应用进行检测	非常有限，通常一个扫描引擎只能同时扫描一个应用	非常有限，扫描器较为耗费资源
部署和使用	非常简单	复杂	复杂

VulHunter产品——VulHunter简介

hardcode相关：
- hardcoded-key
- hardcoded-password

第三方库：
- 第三方库基本信息统计
- 第三方库CVE漏洞
- 第三方库使用情况

安全http header相关：
- hsts-header-missing
- xcontenttype-header-missing
- csp-header-missing
- csp-header-insecure

.....

不安全的跳转：
- unvalidated-forward
- unvalidated-redirect

敏感信息泄露：
- exception 信息泄露
- web server 版本泄露
- 敏感信息经过log泄露
- 敏感信息通过query string传输
- .....

不安全的算法：
- 不安全的加密算法
- 不安全的hash算法
- 不安全的随机数算法

Cookie & Session & Cache：
- cookie-flags-missing
- Httponly
- session-timeout
- session-rewriting
- cache-controls-missing

.....

注入相关：
- xxe
- cmd-injection
- ldap-injection
- log-injection
- reflected-xss
- stored-xss
- Java reflection-injection
- hql-injection
- sql-injection
- Nosql-injection
- xpath-injection
- header-injection

.....

其他：
- clickjacking-control-missing
- parameter-pollution
- autocomplete-missing
- insecure-jsp-access
- verb-tampering
- path-traversal
- trust-boundary-violation
- unsafe-readline
- insecure-socket-factory
- untrusted-deserialization
- Csrf
- Ssrf
- insecure-auth-protocol

.....

VulHunter支持各种漏洞类型的检测

VulHunter产品——VulHunter简介

VulHunter在OWASP Benchmark上的检测结果

Category	CWE #	TP	FN	TN	FP	Total	TPR	FPR	Score
Command Injection	78	126	0	125	0	251	100.00%	0.00%	100.00%
Cross-Site Scripting	79	246	0	209	0	455	100.00%	0.00%	100.00%
Insecure Cookie	614	36	0	31	0	67	100.00%	0.00%	100.00%
LDAP Injection	90	27	0	32	0	59	100.00%	0.00%	100.00%
Path Traversal	22	133	0	135	0	268	100.00%	0.00%	100.00%
SQL Injection	89	272	0	232	0	504	100.00%	0.00%	100.00%
Trust Boundary Violation	501	83	0	43	0	126	100.00%	0.00%	100.00%
Weak Encryption Algorithm	327	130	0	116	0	246	100.00%	0.00%	100.00%
Weak Hash Algorithm	328	129	0	107	0	236	100.00%	0.00%	100.00%
Weak Random Number	330	218	0	275	0	493	100.00%	0.00%	100.00%
XPath Injection	643	15	0	20	0	35	100.00%	0.00%	100.00%
Totals*		**1415**	**0**	**1325**	**0**	**2740**			
Overall Results*							**100.00%**	**0.00%**	**100.00%**

- **True Positive – TP 检出率**
  Tool correctly identifies a real vulnerability
- **False Negative – FN 漏报率**
  Tool fails to identify a real vulnerability
- **True Negative – TN**
  Tool correctly ignores a false alarm
- **False Positive – FP 误报率**
  Tool fails to ignore a false alarm
- **True Positive Rate - TPR**
  TP / (TP + FN)
- **False Positive Rate – FPR**
  FP / (FP + TN)

OWASP Benchmark 免费开源的项目，包含了内置的 **2, 740** 个安全漏洞的测试套件

总结

开源网安 SECZONE GROUP

THANKS

让企业交付更安全的软件

THANK YOU
WeChat：skyzenith